

21-MJ-7091-JCB  
21-MJ-7092-JCB  
21-MJ-7093-JCB  
21-MJ-7094-JCB

**AFFIDAVIT OF SPECIAL AGENT BRYCE J. FERRARA IN SUPPORT OF  
APPLICATION FOR A CRIMINAL COMPLAINT AND SEARCH WARRANTS**

I, Special Agent Bryce Ferrara, being duly sworn, hereby state the following:

1. I am a federal law enforcement officer within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request arrest warrants and search warrants. I am currently employed as a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since January 2019. I am currently assigned to the FBI Boston Violent Crimes Task Force ("VCTF"), which is comprised of personnel from the FBI and Massachusetts State Police, as well as from the Boston, Braintree, Malden, Saugus, Somerville, and Dedham Police Departments.

2. As a Special Agent with the VCTF, I have regularly responded to incidents involving violent encounters. I have also received specialized training regarding investigative techniques, evidence collection, and evidence preservation. My responsibilities include the investigation of possible violations of federal law, including investigation of violent crimes like armed robberies, bank robberies, and threats/extortion. In the course of my career, my investigations have included the use of various surveillance techniques and the execution of various search, seizure, and arrest warrants.

**PURPOSE OF AFFIDAVIT**

3. Based on my training and experience, I know that it is a violation of 18 U.S.C. § 1958(a) to travel in interstate or foreign commerce and/or to use any facilities of interstate or foreign commerce in the commission of murder-for-hire.

4. This affidavit is submitted in support of (1) a criminal complaint charging MASSIMO MARENGHI ("MARENGHI"), DOB xx/xx/1966, with violating 18 U.S.C. § 1958(a), use of interstate commerce or facilities in the commission of murder-for-hire; (2) a search warrant for the person of MARENGHI, as further described in Attachment A-1, annexed

hereto and incorporated herein by reference; (3) a search warrant for the premises located at 104 Pamela Circle, Malden, Massachusetts, as further described in Attachment A-2, annexed hereto and incorporated herein by reference; and (4) a search warrant for a gray 2009 Volvo sedan with Massachusetts registration and license plate number 6NB749, as further described in Attachment A-3, annexed hereto and incorporated herein by reference. Specifically, the purpose of these search warrants is to seize evidence, instrumentalities, fruits of crime, and contraband as more fully described in Attachment B, which is also annexed hereto and incorporated herein by reference.

5. The facts stated herein are based on my own personal involvement in the below-described investigation, as well as from information provided by other law enforcement officers and from certain records. In submitting this affidavit, I have not included each and every fact known to me about this investigation; rather, I am only submitting enough evidence necessary to establish the requisite probable cause.

#### **STATEMENT OF PROBABLE CAUSE**

6. On January 1, 2021, the Northwood (NH) Police Department was contacted by an individual known to law enforcement (hereinafter, “Confidential Source” or “CS”) regarding a conversation that had taken place with Massimo MARENGHI, a resident of Malden, MA, earlier that day.<sup>1</sup> CS reported to police that during their conversation MARENGHI described issues with his wife, including that she had caused a restraining order to be issued against him. CS reported that during their conversation MARENGHI asked if CS would be willing to help kill his wife on his behalf.

---

<sup>1</sup> A member of the Northwood Police Department lives near to, and is personally familiar with, CS. I believe CS and the information he provided during the course of this investigation to be credible based on conversations between that member of the Northwood P.D. and my fellow law enforcement agents and/or officers and because we have been able to corroborate the substance of the information provided by CS. Though CS has some criminal history, his most recent known conviction dates back more than ten years and, regardless, does not cause me to question his credibility with respect to this investigation.

7. On January 1, 2021, the Northwood Police Department referred the report to the Malden (MA) Police Department, and the Malden Police Department contacted the FBI for assistance in the investigation.

8. On January 2, 2021, the FBI contacted and interviewed CS. CS reported that as early as several months prior, MARENGHI had raised the topic of killing his wife with CS. CS explained that at that time he had been able to dissuade MARENGHI from pursuing any additional steps.

9. In text messages between MARENGHI and CS on January 1, 2021, MARENGHI again raised the topic of killing his wife. CS responded that if MARENGHI was serious about having his wife killed, then the cost would be \$10,000 in cash. MARENGHI agreed and provided CS with photographs of his wife, information regarding his wife's employment location and hours, her home address in Malden, a description of her vehicle, and her telephone number. It was after this conversation that CS contacted law enforcement.

10. At the conclusion of his interview with the FBI, CS agreed to assist in the continuing investigation by providing MARENGHI with the name and contact information for someone who MARENGHI would be told could be hired to murder his wife but who, in reality, would be an undercover FBI agent ("UC").

11. On January 13, 2021, at the instruction of the FBI, CS sent MARENGHI a text message, via the cell phone number xxx-xxx-0435, that included the contact phone number for someone who purportedly could assist in MARENGHI's plan to kill his wife. CS also provided MARENGHI with certain words to use when contacting the person to be hired – specifically that MARENGHI refer to the person as "Mrs. Smith," identify himself as someone named "Boston," and inquire about the "construction job."

12. On January 13, 2021, MARENGHI called the phone number that had been provided to law enforcement by CS, that is xxx-xxx-0435. In a recorded conversation, MARENGHI introduced himself as "Boston," asked to speak with "Mrs. Smith," and stated that he was inquiring about a "construction job." Using coded language, the undercover agent

indicated that the job would require “blueprints,” “pictures of the site,” “what time work could start,” and a “preliminary invoice.” MARENGHI and the UC scheduled an in-person meeting for January 20, 2021.

13. On January 18, 2021, the UC sent MARENGHI a text message asking MARENGHI to call the UC. MARENGHI then called the UC and, in a recorded conversation, they discussed meeting on January 20, 2021 at 12:15 PM at a pre-determined location in Portsmouth, NH.

14. On January 20, 2021, MARENGHI and the UC met at the pre-determined location in Portsmouth, NH. MARENGHI arrived in a gray 2009 Volvo sedan with Massachusetts registration and license plate number 6NB749.

15. During the meeting, MARENGHI described a “situation” he needs “taken care of” – that is, his “soon-to-be” ex-wife. The UC asked, “You want to get rid of her?” to which MARENGHI responded, “Yeah, I need to ... to eliminate that problem.” The UC stated, “I mean, we can make it look like an accident ... it is your call.” MARENGHI replied, “Yeah, well, I mean obviously that’s the best way.” At one point, MARENGHI stated, “Well, I just- I just need her out of the way for now.” The UC responded, “OK, well that’s ... that’s totally different. You either want her killed or you don’t.” MARENGHI stated, “Um, I need- I need the problem eliminated.”

16. MARENGHI and the UC discussed a price for the murder-for-hire, \$10,000, and MARENGHI explained that he may need some time to “free up some assets because everything is tied up right now.” During the meeting, MARENGHI provided the UC with a photograph of his wife’s residence. MARENGHI explained in detail the location of the camera outside his wife’s house and described how someone could stand behind the barrels at the end of the driveway such that the person would be hidden from any cameras and out of sight from his wife. MARENGHI further provided a possible exit route likely to evade detection. MARENGHI told the UC that he would bring payment and a photograph of his wife to their next meeting. At the

end of the meeting, MARENGHI and the UC agreed to be in touch again over the next approximately one week.

17. On January 25, 2021, the UC placed one telephone call and sent one text message to MARENGHI. On January 27, 2021, MARENGHI sent a text message to the UC, which said, “call at 5.”

18. On January 27, 2021 and January 28, 2021, MARENGHI and the UC participated in recorded phone conversations during which they discussed payment for the murder-for-hire and the possibility of MARENGHI providing a deposit and additional materials in advance of the murder.

19. During a recorded call on January 28, 2021, MARENGHI agreed to meet the UC on the following day, January 29, 2021, at 10:00 AM at the same, predetermined location in Portsmouth, NH at which they had met on January 20, 2021. MARENGHI agreed to bring a deposit and other materials to the meeting, including a photograph of his wife and information about her work schedule. He agreed to pay the balance at a later date.

20. On January 29, 2021, MARENGHI and the UC met at the pre-determined location in Portsmouth, NH. MARENGHI again arrived in a gray 2009 Volvo sedan with Massachusetts registration and license plate number 6NB749.

21. During the meeting, MARENGHI and the UC discussed details relating to the murder-for-hire. MARENGHI provided the UC with \$1,500 in cash as a deposit for the murder. He explained that the sooner the “demolition job” takes place, the sooner he will be able to pay the balance. He also provided the UC with a photograph of his wife, the hours of operation of her place of business, and a schedule indicating the “best time for the construction work to start.”

22. In each of the above-described telephone and text message-based communications with the UC, MARENGHI called or texted from the number xxx-xxx-0435.

23. In the course of law enforcement’s investigation of MARENGHI, MARENGHI’s residence was determined to be 104 Pamela Circle, Malden, MA, where he is believed to reside with his parents. MARENGHI is known to members of the Malden Police Department, who also

confirm that his address is 104 Pamela Circle. Records from the Massachusetts Registry of Motor Vehicles (“RMV”), including MARENGHI’s driver’s license, list 104 Pamela Circle as his current residence. In their conversations, MARENGHI also informed CS that the 104 Pamela Circle address is his current address.

24. Massachusetts RMV records also list MARENGHI as the owner of a gray 2009 Volvo sedan with Massachusetts registration and license plate number 6NB749. On January 18, 2021, law enforcement officers and/or agents observed the Volvo sedan with plate number 6NB749 parked in front of the residence located at 104 Pamela Circle, Malden, MA. This Volvo sedan is the vehicle that MARENGHI was driving when he arrived at and departed from meetings with the UC on January 20, 2021 and January 29, 2021.

25. Based on my training and experience as an FBI Special Agent, as well as through conversations with other members of law enforcement, I know that people engaged in criminal activity, especially criminal activity that involves phone calls and text messages, frequently possess evidence of that criminal activity on their cell phones. Data relating to such communications, as well as myriad types of additional evidence, including online banking records, internet search history, and social media activity is frequently stored on a cell phone. In this case, MARENGHI is known to have used his cell phone to, among other things, communicate with both the CS and the UC in furtherance of his criminal conduct. I also understand that people regularly possess their cell phones on their person, in their vehicles, and/or in their homes. Most recently, MARENGHI was observed in possession of what is believed to be his cell phone during surveillance conducted on January 29, 2021.

26. Based on my training and experience as an FBI Special Agent, as well as through conversations with other members of law enforcement, I understand that people engaged in criminal conduct regularly use other electronic devices, including but not limited to desktop computers, laptop computers, and tablet devices, in furtherance of their criminal conduct. For example, people use these devices to communicate with co-conspirators, access bank and credit card accounts, effectuate transfers of funds, and conduct research regarding particular people,

locations, and conduct. I understand that people frequently keep computer and other electronic devices on their person, in their vehicles, and/or in their homes.

27. Based on my training and experience as an FBI Special Agent, through conversations with other members of law enforcement, and through my participation in the investigation described in this affidavit, I understand that people who engage in criminal conduct like murder-for-hire may possess hard-copy documents and records, including but not limited to photographs, work schedules, bank and credit card statements, and/or ATM receipts, and that such individuals regularly possess such documents and records on their person, in their vehicles and/or in their homes.

#### **SEIZURE OF COMPUTER EQUIPMENT AND DATA**

28. From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by communicating about them through e-mail, instant messages, and updates to online social-networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online.

29. Based on my training, experience, and information provided by other law enforcement officers, I know that many cell phones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence of communications and evidence that reveals or suggests who possessed or used the device.

30. I am aware of a report from the U.S. Census Bureau that shows that in 2016, among all households nationally, 89 percent had a computer, which includes smartphones, and 81 percent had a broadband Internet subscription. Specifically, in 2016, when the use of

smartphone ownership was measured separately for the first time, 76 percent of households had a smartphone and 58 percent of households had a tablet, and 77 percent of households had a desktop or laptop computer. Further, according to the Pew Research Center, as of 2019, 96 percent of adult Americans own a cellphone, and 81 percent own a cellphone with significant computing capability (a “smartphone”).

31. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the internet. This is true because:

- a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.
- b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase



or delete this evidence because special software is typically required for that task.

- d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.
- e. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- f. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional

information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.

Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide

relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

32. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data

maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media (“computer equipment”) be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

- a. The volume of evidence – storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.
- b. Technical requirements – analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even “hidden” deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a “booby trap.”

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

33. The premises may contain computer equipment whose use in the crime(s) or storage of the things described in these warrants is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of these warrants. If the things described in Attachment Bare of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

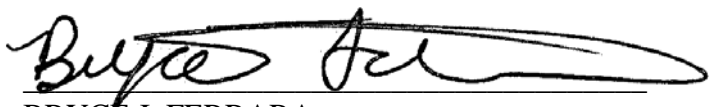
34. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B. If however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

35. These warrants authorize a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed pursuant to these warrants in order to locate evidence, fruits, and instrumentalities described in these warrants. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to these warrants, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

**CONCLUSION**


36. Based on the foregoing, as well as my training and experience and consultation with other special agents and law enforcement officers, I have probable cause to believe that, on or about January 29, 2021, Massimo MARENGHI traveled in interstate commerce, caused another to travel in interstate commerce, used any facility of interstate commerce, and caused another to use any facility of interstate commerce, all with the intent that a murder be committed in violation of the laws of any State or the United States as consideration for the receipt of, or as consideration for a promise or agreement to pay, anything of pecuniary value, in violation of 18 U.S.C. § 1958(a). I also have probable cause to believe that property constituting evidence of the commission of that offense, contraband, fruits of crime, or things otherwise criminally possessed, and property designed or intended for use or which is or has been used as a means of committing a criminal offense will be found: on MARENGHI's person, as described in Attachment A-1; at 104 Pamela Circle, Malden, MA, as described in Attachment A-2; and in the gray 2009 Volvo sedan with Massachusetts registration and license plate number 6NB749, as described in Attachment A-3.

Sworn to under the pains and penalties of perjury.



BRYCE J. FERRARA  
Special Agent, Federal Bureau of Investigation

Subscribed and sworn to via telephone in accordance with  
Fed. R. Crim. P. 4.1 on January 29, 2021.

  
\_\_\_\_\_  
HON. JENNIFER C. BOAL  
UNITED STATES MAGISTRATE JUDGE  
DISTRICT OF MASSACHUSETTS



**ATTACHMENT A-1**  
**PERSON TO BE SEARCHED**

Massimo MARENGHI, year of birth 1966, is pictured below:



**ATTACHMENT A-2**  
**PREMISES TO BE SEARCHED**

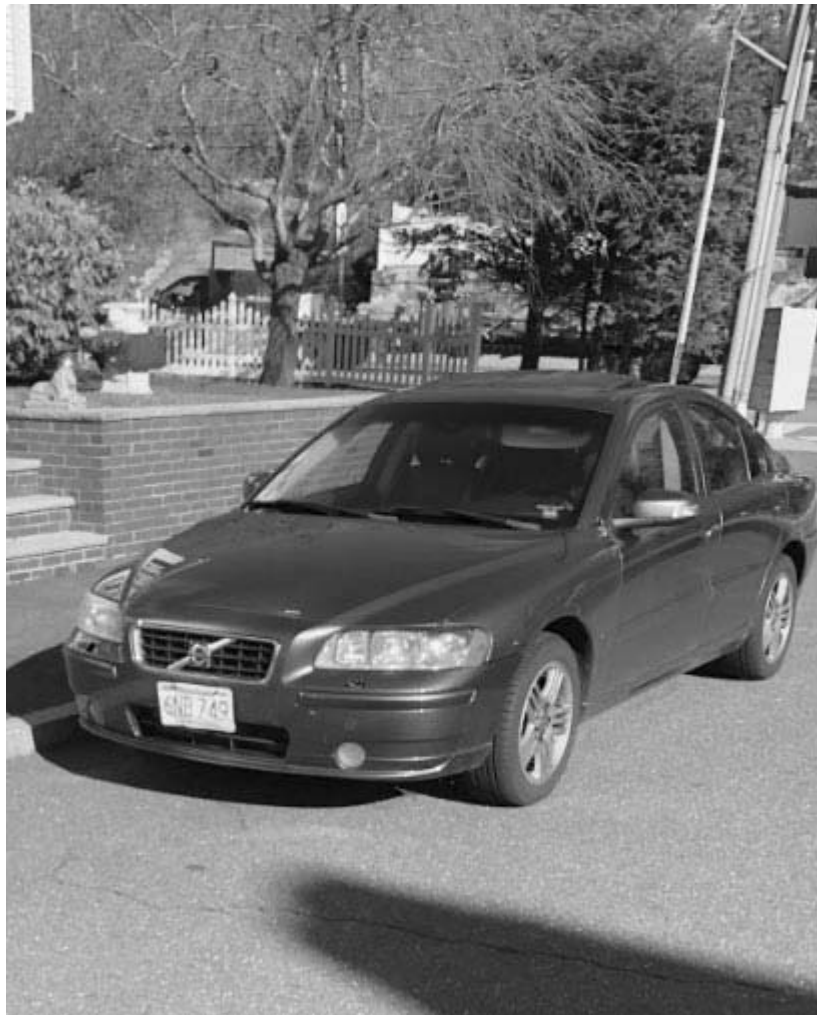
The premises to be searched is located at 104 Pamela Circle, Malden, Massachusetts. The house located at that address has a brick foundation and white vinyl siding. The structure has white and gold-trimmed front doors with the number 104 in gold affixed to the siding to the right of the front door.





**ATTACHMENT A-3**  
**VEHICLE TO BE SEARCHED**

Gray 2009 Volvo sedan with Massachusetts registration and license plate number 6NB749, as depicted in this photo:



**ATTACHMENT B**

**ITEMS TO BE SEIZED**

- I. All records, in whatever form, dating from January 1, 2020 through January 29, 2021 unless otherwise specified, and tangible objects that constitute evidence, fruits, or instrumentalities of 18 U.S.C. § 1958(a), including:
  - A. Records and tangible objects pertaining to the following topics:
    1. Communications with any undercover agents of the Federal Bureau of Investigation between January 1, 2021 and January 29, 2021;
    2. Communications with any other individual regarding the murder, murder-for-hire, and/or plan to murder or otherwise harm the wife of Massimo Marenghi;
    3. Documents and records relating to the wife of Massimo Marenghi, including but not limited to photographs, addresses, vehicle information, work and other schedules, and employment history and records;
    4. Documents and records pertaining to the payment, receipt, transfer, or storage of money or other things of value by Massimo Marenghi, including without limitation:
      - a. Bank, credit union, investment, money transfer, and other financial accounts;
      - b. Credit and debit card accounts;
      - c. Business or personal expenses;
      - d. Income, whether from wages or investments;
      - e. Loans;

5. Records and tangible objects pertaining to the travel or whereabouts of Massimo Marengi between January 1, 2021 and January 29, 2021;
  6. Documents and records relating to murder-for-hire, including bank, credit card, and other financial records, internet or other research, and social media use history and activity; and
  7. Weapons, including firearms and ammunition, as well as documents, records, or communications regarding weapons, the procurement, transfer, ownership, or use of such weapons, that could be used to in the commission of murder or murder-for-hire.
- B. For any computer hardware, computer software, mobile phones, or storage media called for by this warrant or that might contain things otherwise called for by this warrant (“the computer equipment”):
1. Evidence of who used, owned, or controlled the computer equipment;
  2. Evidence of the presence or absence of malicious software that would allow others to control the items, and evidence of the presence or absence of security software designed to detect malicious software;
  3. Evidence of the attachment of other computer hardware or storage media;
  4. Evidence of counter-forensic programs and associated data that are designed to eliminate data;
  5. Evidence of when the computer equipment was used;
  6. Passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;
  7. Records and tangible objects pertaining to accounts held with companies

providing Internet access or remote storage;

8. The identities and aliases of individuals whom participated in the murder-for-hire communications;
9. The locations where planning and/or murder-for-hire occurred;
10. The locations where evidence or other items related to the murder-for-hire were discarded;
11. The methods of communication between participants of murder-for-hire, including the telephone numbers, messaging applications, and social media accounts used by the individuals;
12. The substance of communications regarding the planning, execution, and/or discussion of the murder-for-hire;
13. The substance of communications regarding the acquisition, disposal, and/or discussion of clothing, firearms, and other items intended to be used before, during, or after the commission of the murder-for-hire;
14. The substance of communications regarding firearms and/or ammunition;
15. The substance of communications regarding money or other items as payment for the murder-for-hire;
16. Photographs of items or information related to the planning, execution, or discussions related to the murder-for-hire;
17. The relationship between the users of the Target Devices and other identified co-conspirators; and
18. The identity, location, and travel of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the crimes listed above.

- C. Records and tangible objects relating to the ownership, occupancy, or use of the premises to be searched (such as utility bills, phone bills, rental or lease agreements, rent payments, mortgage bills and/or payments, photographs, insurance documentation, receipts, and check registers); and
- II. All computer hardware, computer software, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraph I.

### **DEFINITIONS**

For the purpose of this warrant:

- A. “Computer equipment” means any computer hardware, computer software, mobile phone, storage media, and data.
- B. “Computer hardware” means any electronic device capable of data processing (such as a computer, smartphone, cell/mobile phone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. “Computer software” means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

- D. “Storage media” means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).
- E. “Data” means all information stored on storage media of any form in any storage format and for any purpose.
- F. “A record” is any communication, representation, information or data. A “record” may be comprised of letters, numbers, pictures, sounds or symbols.

### **RETURN OF SEIZED COMPUTER EQUIPMENT**

If the owner of the seized computer equipment requests that it be returned, the government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the government determines that some or all of this equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy’s authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If computer equipment cannot be returned, agents will make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, or personally-identifying information of victims; or the fruits or instrumentalities of crime.

For purposes of authentication at trial, the Government is authorized to retain a digital copy of all computer equipment seized pursuant to this warrant for as long as is necessary for authentication purposes.